REMARKS

The Office Action dated December 13, 2007 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Applicants gratefully acknowledge the indication in the Office Action that claims 6-9, 13-15, 17, and 27 would be allowable if rewritten into independent form. However, as discussed below, Applicants respectfully submit that these claims are allowable in their present form. In accordance with the foregoing, claims 26 and 32-36 have been amended to more particularly point out and distinctly claim the subject matter of the invention. No new matter is being presented, and approval and entry are respectfully requested.

Claims 1-9, 13-15, 17, 21, and 23-38 are pending and under consideration.

REJECTION UNDER 35 U.S.C. § 103:

Claims 2-3, 24-26, and 32-38 were rejected under 35 USC §103(a) as being obvious in view of RFC 2977, U.S. Application No. 2002/065785 to Tsuda ("Tsuda"), and U.S. Patent No. 6,751,459 to Lee et al. ("Lee"). The Office Action took the position that RFC 2977, Tsuda, and Lee disclose all aspects of claims 2-3, 24-26, and 32-38. It is respectfully asserted that, for at least the reasons provided herein below, RFC 2977,

Tsuda, and Lee fail to teach or suggest the recitations of the pending claims. Reconsideration is requested.

Independent claim 3 recites a method including maintaining in a mobile communication system subscriber's location information, and receiving a message from subscriber's user equipment, the message including subscriber's location information and indicating that an address of a certificate provisioning gateway for certificate issuance. Delivery procedure in a visited network is requested by the subscriber's user equipment, and the certificate provisioning gateway serving at least one certificate authority. The method also includes checking, in response to receiving the message, whether or not the location information in the message corresponds to the location information maintained in the system, and using the maintained location information for determining the address of the certificate provisioning gateway if the maintained location information does not correspond to the location information in the message.

Independent claim 24, from which claims 6-9 and 13 depend, recites a method including maintaining in a mobile communication system subscriber's location information, and receiving a message from subscriber's user equipment. The message including subscriber's location information and indicating that an address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment. The certificate provisioning gateway serves at least one certificate authority. The method includes checking, in response to receiving the message, whether or not the location information in the message

corresponds to the location information maintained in the system, and if the maintained location information corresponds to the location information in the message, determining on the basis of the subscriber's location information the address of the certificate provisioning gateway. If the maintained location information does not correspond to the location information in the message, the method includes sending an error indication by using the maintained location information.

Independent claim 25, from which claim 27 depends, recites a method including maintaining in a mobile communication system subscriber's location information, and receiving a message from subscriber's user equipment, the message comprising subscriber's location information and indicating that an address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment, the certificate provisioning gateway serving at least one certificate authority. The method includes checking, in response to receiving the message, whether or not the location information in the message corresponds to the location information maintained in the system, and determining, on the basis of the subscriber's location information the address of the certificate provisioning gateway; if the location information in the message corresponds to the maintained location information. The method includes using the location information in the message if the location information in the message does not correspond to the maintained location information.

Independent claim 26, from which claims 14, 15, and 17 depend, recites a method including maintaining in a mobile communication system subscriber's location information, receiving a message from subscriber's user equipment. The message comprises subscriber's location information and indicating that an address of a certificate provisioning gateway for certificate issuance. Delivery procedure in a visited network is requested by the subscriber's user equipment, and the certificate provisioning gateway serving at least one certificate authority. The method includes checking, in response to receiving the message, whether or not the location information in the message corresponds to the location information maintained in the system. The method further includes if the location information in the message corresponds to the maintained location information, determining on the basis of the subscriber's location information the address of the certificate provisioning gateway, and if the location information in the message does not correspond to the maintained location information, sending an error indication by using the location information in the message.

Independent claim 32 recites an apparatus, including a processor configured to serve a certificate authority in a mobile communication system, to determine, in response to receiving from subscriber's user equipment a message indicating a request for an address of another certificate provisioning gateway for certificate issuance and delivery procedure. The message includes an address of the other certificate provisioning gateway, an address of the other certificate provisioning gateway on the basis of subscriber's location information maintained in and obtained from the mobile

communication system. The processor is also configured to check whether or not the address in the message corresponds to the address determined on the basis of the location information, and if they do not correspond to each other, to use the address determined on the basis of the location information.

Independent claim 33 recites an apparatus, including a processor configured to serve a certificate authority in a mobile communication system, and to check, in response to receiving from subscriber's user equipment a message. The message includes subscriber's location information and indicates a request for an address of another certificate provisioning gateway for certificate issuance and delivery procedure in a visited network, whether or not the location information in the message corresponds to subscriber's location information maintained in and obtained from the system. The processor is also configured to use the maintained location information to determine the address of the other certificate provisioning gateway if the maintained location information does not correspond to the location information in the message.

Independent claim 34 recites an apparatus, including a processor configured to serve a certificate authority in a mobile communication system, and to check, in response to receiving from subscriber's user equipment a message including subscriber's location information and indicating that an address of another certificate provisioning gateway for certificate issuance. Delivery procedure in a visited network is requested, whether or not the location information in the message corresponds to subscriber's location information maintained in and obtained from the system. If the location information in the message

corresponds to the maintained location information, the processor is also configured to determine an address of the other certificate provisioning gateway on the basis of the subscriber's location information, and, if the maintained location information does not correspond to the location information in the message, to send an error indication by using the maintained location information.

Independent claim 35 recites an apparatus, including a processor configured to serve a certificate authority in a mobile communication system, to check, in response to receiving from subscriber's user equipment a message. The message includes subscriber's location information and indicating a request for an address of another certificate provisioning gateway for certificate issuance and delivery procedure in a visited network, whether or not the location information in the message corresponds to the location information maintained in the system, and to use the location information in the message to determine the address of the other certificate provisioning gateway if the location information does not correspond to the maintained location information.

Independent claim 36 recites an apparatus including a processor configured to serve a certificate authority in a mobile communication system, to check, in response to receiving from subscriber's user equipment a message. The message includes subscriber's location information and indicating a request for an address of another certificate provisioning gateway for certificate issuance and delivery procedure in a visited network, whether or not the location information in the message corresponds to subscriber's location information maintained in and obtained from the system. The

processor is also configured to determine on the basis of the subscriber's location information the address of the other certificate provisioning gateway, if the location information in the message corresponds to the maintained location information, and if the location information does not correspond to the maintained location information, to send an error indication by using the location information in the message.

As will be discussed below, RFC 2977, Tsuda, and Lee fail to disclose or suggest the elements of any of the presently pending claims.

RFC 2977 generally describes a mobile IP and requirements which would have to be supported by a Authentication, Authorization, Accounting (AAA) service to aid in providing mobile IP services. The basic model described in section 3 of RFC 2977 a client belonging to one administrative domain (called home domain) having to use resources provided by another administrative domain (called foreign domain). An agent in the foreign domain that attends to the client's request (call the agent the "attendant") is likely to require that the client provide some credentials that can be authenticated before access to the resources is permitted. The attendant is expected to consult an authority (typically in the same foreign domain) in order to request proof that the client has acceptable credentials.

RFC 2977 identifies the following requirements that have to be supported: Each local attendant has to have a security relationship with the local AAA server (AAAL), the local authority has to share, or dynamically establish, security relationships with external authorities that are able to check client credentials; the attendant has to keep state for

pending client requests while the local authority contacts the appropriate external authority; since the mobile node may not necessarily initiate network connectivity from within its home domain, it MUST be able to provide complete, yet unforgeable credentials without ever having been in touch with its home domain; and intervening nodes (e.g., neither the attendant or the local authority (AAAL) or any other intermediate nodes) MUST NOT be able to learn any (secret) information which may enable them to reconstruct and reuse the credentials.

However, other than listing requirements, RFC 2977 does not teach or suggest that a message is received from a subscriber's user equipment, where the message would be configured to indicate "that an address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment, the certificate provisioning gateway serving at least one certificate authority, the message further comprising the address of the certificate provisioning gateway," as recited in independent claim 2 and similarly recited in independent claims 3, 24-26, and 32-36. RFC 2977 does not provide a message that would indicate an address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network. The description provided in RFC 2977 of various listings of requirements to roaming and related to basic IP connectivity, would not enable a person of ordinary skill in the art to arrive at the claimed invention. Section 4 of RFC 2977 simply lists requirements on AAA services including AAA server MUST be able to obtain, or to coordinate the allocation of, a suitable IP address for the customer, upon

request by the customer; and AAA servers MUST be able to identify the client by some means other than its IP address. However, there is no teaching or suggestion regarding the address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment.

Also, section 5 of RFC 2977 is limited to submitting that the AAA server MUST also be able to validate certificates provided by the mobile node and provide reliable indication to the foreign agent. However, similar to other portions of RFC 2977, section 5 does not teach or suggest the particular features of independent claim 2 reciting the "address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment." Furthermore, neither sections 3-5 of RFC 2977 teach or suggest, at least, "determining, in response to receiving the message, on the basis of the subscriber's location information, an address of the certificate provisioning gateway," as recited in independent claim 2 and similarly recited in independent claims 3, 24-26, and 32-36.

RFC 2997 fails to teach a certificate provisioning gateway (and a certificate authority), and, therefore, it cannot disclose any feature relating to the certificate provisioning gateway.

If home/foreign authorities are considered as certificate provisioning gateways, although not admitted or suggested to have that kind of functionality by RFC 2977, the user equipment need not request for their addresses according to the description of RFC 2977. The user equipment knows its home authority address. Further, the user

- 22 -

equipment establishes no direct connection to a foreign authority but uses an attendant, whose address the user equipment knows (otherwise, the user equipment could not send any messages to attendant and the user equipment would not obtain a service). The attendant then provides different services in the foreign network, the services including contacts to home authority. According to RFC 2977, the address of the attendant is the only address needed for the foreign network.

As correctly recognized by the Office Action, RFC 2977 fails to teach or suggest, "checking whether or not the address in the message corresponds to the address determined on the basis of the location information; and if they do not correspond to each other, using the address determined on the basis of the location information," as recited in independent claim 2 and similarly recited in independent claims 3, 24-26, and 32-36. To resolve the deficiencies of RFC 2977, the Office Action relied on Tsuda and Lee. However, as will be discussed below, Tsuda and Lee fail to cure the deficiencies of RFC 2977.

Tsuda generally describes a function for carrying out AAA processing and authentication and accounting processes carried out between AAA function (AAAM) on a mobile node and a visited network or the mobile node and a home network. See paragraph [0054]. When the mobile node is connected to the visited network, for example, the mobile node 1010 transmits a registration request to the home agent or the AAAH server according a Mobile IP protocol. See FIG. 1 and paragraphs [0061]-[0065].

Furthermore, Tsuda describes that a foreign agent sends periodically an advertisement including its own address (S101), and, thus, the mobile terminal receives the address without requesting. See, at least, FIGS. 10 and 11 of Tsuda. In Tsuda, when the mobile terminal notices that it has changed sub-network, it sends a registration request S102 to the foreign agent using the address the mobile terminal received in the advertisement. Then, the mobile terminal is authenticated and keys changed, such keys being used to encrypt communication.

Lee generally describes a method and apparatus for nomadic computing by means of transparent virtual networking, information storage, and mobility when the user is traveling from one location to another and/or using different computer platforms or operating modes. Personal mobility domain name service (PMDNS) is originally designed to provide personal mobility via a personal identifier. Because of generic system architecture which uses the Internet as backbone, interoperating with existing access networks, it is also wise to provide nomadic computing services.

However, similar to RFC 2977 alone, a combination of RFC 2977, Tsuda, and Lee would not teach or suggest all the recitations of independent claims 2, 3, 24-26, and 32-36. For instance, RFC 2977, Tsuda, and Lee are silent as to teaching or suggesting, at least, "receiving a message from subscriber's user equipment, said message indicating that **an address of a certificate provisioning gateway for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment**, the certificate provisioning gateway serving at least one certificate

authority," as recited in independent claim 1. (Emphasis added) In addition, Tsuda and Lee do not teach or suggest that a message is received from a user equipment requesting the address of a network element. Rather, Tsuda describes sending from a network node advertising messages containing an address without any request from the user equipment.

Also, Tsuda discloses that AAA servers are for authentication, authorization, and accounting, (See paragraph [0004]) and that AAA-H server locates in a home network and AAA-F server in a visited network. Further, Tsuda discloses in paragraph [0186] a certificate authority as a separate entity, not included in the AAA servers, and states that the certificate authority may be used in addition to the AAA servers. Thus, Tsuda describes that AAA-servers cannot be interpreted as certificate authorities. Lee is completely devoid of any teaching or suggestion regarding AAA servers and certificate authorities.

Furthermore, independent claim 2 recites a certificate issuance and the certificate provisioning gateway serving at least one certificate authority, whereas Tsuda and Lee relates to routing services. Tsuda and Lee describes how to find a mobile terminal when the terminal has a fixed IP address used as its identification, but the actual IP address of the terminal depends on the terminal's location. Clearly, RFC 2977, Tsuda, and Lee are silent as to teaching or suggesting that a user equipment could use a certificate issuance services of a visited network, or of another network than a home network of the user equipment. On the contrary, Tsuda describes for example in paragraph [0056] to always contact the AAA server in the home network to authenticate the user.

Furthermore, certificate authorities are provided as separate entities in the present application, and for one skilled in the art a certificate authority is a trusted third party issuing certificates. Thus, one skilled in the art would not interpret an authentication, authorization, and accounting server as a certificate authority issuing certificates, and none of the cited references describe such feature.

A combination of RFC 2977, Tsuda, and Lee would teach away from the claimed invention because the combination would teach all network-related data should be sent in advertise messages. As done in the Office Action, providing that a combination of RFC 2977, Tsuda, and Lee would teach the recitations of the claims is purely based on hindsight. "To support the conclusion that the claimed combination is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed combination. It is to be noted that simplicity and hindsight are not proper criteria for resolving the issue of obviousness." *Ex Parte Clapp*, 227 USPQ 972, 973 (B.P.A.I. 1985).

For similar reasons, RFC 2977, Tsuda, and Lee do not teach or suggest, "determining, **in response to receiving the message**, on the basis of the subscriber's location information, an address of the certificate provisioning gateway," emphasis added, as recited in independent claim 2 and similarly recited in independent claims 3, 24-26, and 32-36.

Regarding independent claims 6 and 14, paragraph [0069] of Tsuda generally describes accounting and disclosing how subscribers are billed and paragraph [00186] of

Tsuda describes that public key information or certificate authority may be used in addition to authentication. However, Tsuda fails to teach or suggest that "an address of a certificate provisioning gateway via which the certificate issuance service is provided in the other network, the certificate provisioning gateway serving at least one certificate authority, a public key required for the certificate issuance service in the other network, and an indication of the protocol required for the certificate issuance service in the other network," as recited in independent claims 6 and 14. RFC 2977 and Lee are devoid of any teaching or suggestion providing such features. Based on the description of Tsuda, the certificate authority used locates the home network, or the public key is used for the home network, and, therefore, one skilled in the art would assume that they are stored in the user equipment.

In view of the descriptions of Tsuda and Lee, these references do not cure the deficiencies of RFC 2977. A combination of RFC 2977, Tsuda, and Lee would fail to teach or suggest all the recitations of the present claims. Instead, the combination of RFC 2977, Tsuda, and Lee would simply list requirements that need to be supported by a AAA service to aid in providing mobile IP services, where the mobile IP network could have home zone information and provide home zone services in a subnet using an address of AAAH. However, there is no teaching or suggestion in the combination of RFC 2977, Tsuda, and Lee providing receiving a message from subscriber's user equipment, said message indicating that an address of a network node for certificate issuance and delivery procedure in a visited network is requested by the subscriber's user equipment and

transmitting after the authentication via an authenticated channel to subscriber's user equipment at least part of information required for a certificate of issuance service in another network than a home network of the subscriber.

Accordingly, in view of the foregoing, it is respectfully requested that independent claims 2, 3, 24-26, and 32-36 and related dependent claims be allowed.

CONCLUSION:

In view of the above, Applicant respectfully submits that the claimed invention recites subject matter which is neither disclosed nor suggested in the cited prior art. Applicant further submits that the subject matter is more than sufficient to render the claimed invention unobvious to a person of skill in the art. Applicant therefore respectfully requests that each of claims 2-3, 24-26, and 32-38 be found allowable and, along with allowed claims 6-9, 13-15, 17, and 27, this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time.

Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Alicia M. Choi
Registration No. 46,621

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

AMC:dc

Enclosures: Petition for Extension of Time
              Check No. 18971